



General Assembly

February Session, 2012

Raised Bill No. 5427

LCO No. 1909

01909_____JUD

Referred to Committee on Judiciary

Introduced by:
(JUD)

**AN ACT CONCERNING NOTICE TO THE ATTORNEY GENERAL OF
DATA SECURITY BREACHES INVOLVING THE DISCLOSURE OF
PERSONAL INFORMATION.**

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. Section 36a-701b of the general statutes is repealed and
2 the following is substituted in lieu thereof (*Effective October 1, 2012*):

3 (a) For purposes of this section, "breach of security" means
4 unauthorized access to or acquisition of electronic files, media,
5 databases or computerized data containing personal information when
6 access to the personal information has not been secured by encryption
7 or by any other method or technology that renders the personal
8 information unreadable or unusable; "personal information" means an
9 individual's first name or first initial and last name in combination
10 with any one, or more, of the following data: (1) Social Security
11 number; (2) driver's license number or state identification card
12 number; or (3) account number, credit or debit card number, in
13 combination with any required security code, access code or password
14 that would permit access to an individual's financial account. "Personal
15 information" does not include publicly available information that is

16 lawfully made available to the general public from federal, state or
17 local government records or widely distributed media.

18 (b) Any person who conducts business in this state, and who, in the
19 ordinary course of such person's business, owns, licenses or maintains
20 computerized data that includes personal information, shall [disclose]
21 provide notice of any breach of security following the discovery of the
22 breach to the Attorney General immediately following the discovery of
23 the breach of security and to any resident of this state whose personal
24 information was, or is reasonably believed to have been, accessed by
25 an unauthorized person through such breach of security. [Such
26 disclosure] Notice to a resident of this state shall be made without
27 unreasonable delay, subject to the provisions of subsection (d) of this
28 section and the completion of an investigation by such person to
29 determine the nature and scope of the incident, to identify the
30 individuals affected, or to restore the reasonable integrity of the data
31 system. [Such notification] Notification to affected residents shall not
32 be required if, after an appropriate investigation and consultation with
33 relevant federal, state and local agencies responsible for law
34 enforcement, the person reasonably determines that the breach will not
35 likely result in harm to the individuals whose personal information has
36 been acquired and accessed.

37 (c) Any person that maintains computerized data that includes
38 personal information that the person does not own shall notify the
39 owner or licensee of the information of any breach of the security of
40 the data immediately following its discovery, if the personal
41 information was, or is reasonably believed to have been accessed by an
42 unauthorized person.

43 (d) Any notification to a resident of this state required by this
44 section shall be delayed for a reasonable period of time if a law
45 enforcement agency determines that the notification will impede a
46 criminal investigation and such law enforcement agency has made a
47 request that the notification be delayed. Any such delayed notification

48 shall be made after such law enforcement agency determines that
49 notification will not compromise the criminal investigation and so
50 notifies the person of such determination. Nothing in this section shall
51 relieve any person of the obligation to notify the Attorney General of a
52 breach of security immediately following the discovery of such breach
53 of security.

54 (e) Any notice to a resident, owner or licensee required by the
55 provisions of this section may be provided by one of the following
56 methods: (1) Written notice; (2) telephone notice; (3) electronic notice,
57 provided such notice is consistent with the provisions regarding
58 electronic records and signatures set forth in 15 USC 7001; (4)
59 substitute notice, provided such person demonstrates that the cost of
60 providing notice in accordance with subdivision (1), (2) or (3) of this
61 subsection would exceed two hundred fifty thousand dollars, that the
62 affected class of subject persons to be notified exceeds five hundred
63 thousand persons or that the person does not have sufficient contact
64 information. Substitute notice shall consist of the following: (A)
65 Electronic mail notice when the person [, business or agency] has an
66 electronic mail address for the affected persons; (B) conspicuous
67 posting of the notice on the web site of the person [, business or
68 agency] if the person maintains one; and (C) notification to major state-
69 wide media, including newspapers, radio and television.

70 (f) Any person that maintains such person's own security breach
71 procedures as part of an information security policy for the treatment
72 of personal information and otherwise complies with the timing
73 requirements of this section, shall be deemed to be in compliance with
74 the security breach notification requirements of this section pertaining
75 to affected residents, owners and licensees, provided such person
76 notifies subject persons in accordance with such person's policies in the
77 event of a breach of security. Any person that maintains such a
78 security breach procedure pursuant to the rules, regulations,
79 procedures or guidelines established by the primary or functional
80 regulator, as defined in 15 USC 6809(2), shall be deemed to be in

81 compliance with the security breach notification requirements of this
82 section pertaining to affected residents, owners and licensees,
83 provided such person notifies subject persons in accordance with the
84 policies or the rules, regulations, procedures or guidelines established
85 by the primary or functional regulator in the event of a breach of
86 security of the system.

87 (g) Failure to comply with the requirements of this section shall
88 constitute an unfair trade practice for purposes of section 42-110b and
89 shall be enforced by the Attorney General.

This act shall take effect as follows and shall amend the following sections:		
Section 1	October 1, 2012	36a-701b

Statement of Purpose:

To require that persons who own, license or maintain computerized data that includes personal information immediately notify the Attorney General in the event of a breach of security relating to such data.

[Proposed deletions are enclosed in brackets. Proposed additions are indicated by underline, except that when the entire text of a bill or resolution or a section of a bill or resolution is new, it is not underlined.]